Gênero & Direito
Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 6 - Nº 03 - Ano 2017 (Spanish Edition)
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

CIBER CRÍMENES, GÉNERO Y DERECHOS HUMANOS PREVENCIÓN DEL CIBERDELITO

Laura López Díaz[1]
Josefina De la Cruz Izquierdo[2]
Erika Yunuen Morales Mateos[3]
María Arely López Garrido[4]

Resumen: Es importante prevenir los delitos informáticos y garantizar la privacidad, ya que hoy en día han aumentado los delitos y cada día son más graves. La privacidad constituye una preocupación tanto para los individuos como para las corporaciones, es por ello que se necesita atacar dichos delitos en la medida de lo posible. La cantidad de datos e información digital ha aumentado con el inicio del internet y el adentramiento en la red mundial; casi toda esta comunicación es lícita, pero las computadoras, redes, telecomunicaciones y la información electrónica también se utilizan para cometer delitos y perfeccionar las técnicas delincuenciales, creciendo nuevas formas de robo y sabotaje de la información. Los avances tecnológicos les han permitido tanto a los delincuentes, como a los grupos criminales el obtener un medio efectivo por el cual conseguir víctimas que caigan en sus redes y que se expongan en situaciones de peligro. Ninguna persona elige ser víctima de un delito, sólo se expone por falta de precaución y desconocimiento de sus derechos. Estos delitos se enfocan en afectar la privacidad de corporaciones y jaqueo de información en el ámbito económico. lo que resulta en daños económicos a empresas y particulares y que les impone gastos en la protección de información y restauración de la información pérdida. También existen afectaciones que afectan a la sociedad en general, especialmente al grupo vulnerable de las mujeres, pues entre esos delitos se hallan aquellos que enfatizan su denigración y la violencia existente en países como México, con una cultura tradicionalista y

[1] Dra. en Educación. Profesora Investigadora de la Universidad Juárez Autónoma de Tabasco
[2] Dra. en Educación. Profesora Investigadora de la Universidad Juárez Autónoma de Tabasco
[3] Dra. en Sistemas Computacionales. Profesora Investigadora de la Universidad Juárez Autónoma de Tabasco
[4] Dra. en Sistemas Computacionales. Profesora Investigadora de la Universidad Juárez Autónoma de Tabasco

marcadamente patriarcal, como la del acoso virtual, el sexting, la prostitución y trata, entre otros.

Palabras claves: ciberdelito, pharming, género

Abstract: It is important to prevent cybercrimes and to ensure privacy, because crime has grown today, and every day is more serious. Privacy is a concern for both individuals and corporations. It is necessary to attack such crimes as soon as possible. The amount of data and digital information has increased with the initiation of the internet and the penetration in the global network; almost all of this communication is lawful, but computers, networks, telecommunications and electronic information are also used to commit crimes and perfect criminal techniques, growing new forms of information theft and sabotage. Technological advances have allowed both delinquents and criminal groups to obtain an effective mean by which victims can fall into their networks and expose themselves to dangerous situations. No person chooses to be a victim of a crime, only exposed for lack of caution and ignorance of their rights. These crimes focus on affecting the privacy of corporations and hacking information in the economic area. It results in economic damage to businesses and individuals and imposes on them expenses in the protection of information and restoration of lost information. There are also affectations that impact society in general, especially to the vulnerable group of women. Among these crimes are those that emphasize their denigration and the existent violence that happens in Mexico, which has a traditional and patriarchal culture such as virtual harassment, sexting, prostitution and trafficking, among others.

Keywords: Cibercrime, pharming, gender

INTRODUCCIÓN

El Internet ha abierto un espacio en donde las expresiones pueden realizarse de manera libre; esta libertad se ejerce e interactúa más rápido y fácil, lo que implica una dificultad para ir creando leyes de protección a la seguridad y privacidad, principalmente en las redes sociales, que es el espacio en donde más interacción existe y en donde existe más peligro y vulnerabilidad; pues tanto la intimidad, privacidad, buen nombre y libertad de expresión se ven

afectados y por lo general no saben qué hacer para defenderse de un ataque (Castillo Vargas, s. f.)

La legislación busca el implementar castigos acordes a los delitos que día a día se realizan. Estas leyes, tienen la característica de enfocarse en situaciones referentes a la seguridad comercial y estatal, pero dejan de lado la cuestión social.

La creación de leyes que busca el proteger la seguridad nacional se utiliza como una restricción de los derechos individuales referentes a la privacidad o la que se enfoca a la libertad de expresión. Uno de los requerimientos que actualmente se le solicita a los legisladores es el de analizar el impacto que dicha legislación tendrá sobre los ciudadanos, si facilitara el empoderamiento de grupos vulnerables, en especial de las mujeres.

Cada que se habla o menciona el ciberdelito, se piensa en delitos como fraude, robo de números de tarjetas de crédito o hacking, en este aspecto los ciberdelitos se clasifican en contra de la persona como los acosos cibernéticos; los cometidos contra la propiedad, como el hacking; o los delitos cometidos contra el gobierno como el que implementan los terroristas usando medios electrónicos.

DELITOS QUE AFECTAN LA SEGURIDAD COMERCIAL Y SUGERENCIAS DE PROTECCIÓN.

Con el objetivo de ayudar a la prevención de los ciberdelitos, los usuarios deben proteger sus sistemas informáticos y datos (transacciones y sus protocolos de comunicación) contra los ataques, haciendo uso de las tecnologías de seguridad con ciertas configuraciones para su protección segura.

Encontramos que existen Técnicas de Suplantación que consisten en la apropiación de los derechos y facultades propias de la persona suplantada. (Por ejemplo, acceder sin consentimiento a la cuenta de una red social). Phishing es un término informático utilizado para denominar el fraude por suplantación de identidad. El término phishing procede de la palabra inglesa fishing (pesca) haciendo alusión a "picar el anzuelo".

Pharming de la cual el ciberdelicuente infecta el ordenador del usuario de forma que se acaba redireccionando el tráfico web de una página legitima, utilizada habitualmente por el usuario, hacia otra página falsa creada por el ciberdelincuente.

SMiShing aunque menos habitual en la actualidad debido al menor

uso de SMS entre los usuarios, como variante del phishing, se configura como un tipo de delito o actividad criminal que emplea técnicas de ingeniería social y mensajes de texto dirigidos a los usuarios de telefonía móvil.

El acuerdo más amplio que existe para proteger los datos e información de las empresas es el de la Seguridad Multilateral, que implica el proporcionar seguridad a todas las partes interesadas como protección a particulares, evitar conflictos de seguridad, usar la tecnología para la seguridad multilateral que tiene la posibilidad de liberar a los usuarios de sistemas de TIC de la falta de autodeterminación, resultante de su falta de seguridad.

Otras requieren cooperación bilateral, por ejemplo la cooperación entre las dos partes de una comunicación. Algunas requieren la cooperación trilateral. Un ejemplo es el de las firmas digitales legalmente vinculantes, que requieren no sólo la cooperación de las partes comunicantes (al menos dos), sino además al menos una tercera parte depositaria para la certificación de las claves públicas. Para otras tecnologías podría ser incluso necesaria la cooperación multilateral entre un gran número de partes independientes.

En su investigación Pfitzmann, (2000) menciona que las Tecnologías Unilaterales son aquéllas en las que cada parte puede decidir por sí misma. Por lo tanto, no se necesita ni coordinación ni negociación en lo referente a su uso. Las tecnologías unilaterales importantes para la seguridad multilateral son:

- Herramientas para ayudar incluso a usuarios sin experiencia a formular todos sus objetivos de protección, en caso necesario para todas y cada una de las aplicaciones o para todas y cada una de las acciones (Pfitzmann y Wolf, (2000).
- Dispositivos (portátiles) que son seguros para sus usuarios con el fin de programar la seguridad. Los dispositivos necesitan al menos una protección física mínima que comprenda un input/output directo con sus usuarios (Pfitzmann, (1999) y, si son multiuso, un sistema operativo que proporcione un fino control de acceso y administración de los derechos de las aplicaciones, de acuerdo con el principio de privilegio

mínimo. Esto es esencial para limitar la difusión de virus denominados "caballos de Troya", y evitar por completo los virus informáticos.

- Codificación criptográfica de los medios locales de almacenamiento para ocultar y/o autenticar sus contenidos.
- Ocultación de datos secretos en contenidos multimedia locales o en el sistema local de archivo utilizando técnicas esteganográficas, no sólo para ocultar los contenidos de los datos secretos, sino también su propia existencia.
- Impresión de watermark o de huellas digitales en los datos digitales utilizando técnicas esteganográficas para ayudar a demostrar las infracciones del derecho de autor o de copyright.
- Utilizar solamente software cuyo código de fuente esté publicado y bien comprobado o cuya seguridad esté certificada por una tercera parte depositaria que tenga acceso al código de fuente completo y a todas las herramientas utilizadas para la generación del código.

La mejor técnica es combinar ambos planteamientos teniendo en consideración el software en la mayor medida posible. Solamente utilizando al menos uno de estos dos planteamientos se podrá tener una certeza razonable de que el software que se emplea no contiene virus. Más o menos lo mismo puede decirse del hardware, donde también se necesitan todas las fuentes y herramientas utilizadas para su diseño y producción para comprobar la ausencia de "caballos de Troya".

Las opciones de seguridad unilateral incluyen dispositivos portátiles seguros, codificación criptográfica de los datos almacenados localmente, impresión de watermark y utilización de software de fuente abierta o certificado.

Las tecnologías bilaterales sólo pueden utilizarse si las partes de una comunicación cooperan entre sí. Esto quiere decir que se necesita cierto grado de coordinación y de cooperación en lo que se refiere a su uso.

Las tecnologías bilaterales incluyen herramientas para negociar los mecanismos de seguridad y mecanismos criptográficos y esteganográficos para proteger el contenido.

Las tecnologías bilaterales importantes para la seguridad multilateral son:

- Herramientas para negociar los objetivos de protección y los mecanismos de seguridad bilaterales (Pfitzmann, (1998)
- Criptografía para conseguir la confidencialidad y la integridad del contenido de la comunicación
- Esteganografía para obtener la ocultación, es decir el secreto del contenido de una comunicación confidencial

Las tecnologías trilaterales sólo pueden utilizarse si está implicada una tercera parte que cumpla una tarea específica para las otras partes participantes. Esto significa que se necesita mayor coordinación y negociación en lo referente a su uso en comparación con las tecnologías unilaterales y en la mayoría de los casos, también con las bilaterales. Las tecnologías trilaterales importantes para la seguridad multilateral son:

- Herramientas para negociar los mecanismos de seguridad trilateral, por ejemplo para la responsabilidad.
- Una infraestructura de claves públicas (PKI) para proporcionar a los usuarios las claves públicas certificadas de otros usuarios, a fin de comprobar sus firmas digitales y dar a los usuarios la facultad de revocar su clave pública propia si ha sido comprometida la clave privada correspondiente.
- Puertas de seguridad para crear una interfaz entre incompatibilidades en mecanismos o detalles de seguridad. Las puertas de seguridad funcionan bien para los mecanismos de integridad y de responsabilidad, pero son de valor dudoso para los mecanismos de confidencialidad y de anonimato. Por supuesto las puertas de seguridad no pueden crear una interfaz entre incompatibilidades en objetivos de protección.
- Mecanismos para proporcionar seudónimos digitales, es decir, una combinación adecuada de anonimato y de responsabilidad (Chaum, (1981). En particular, existen mecanismos para transferir de forma segura firmas

(que expresan autorización, llamadas credenciales) entre diferentes seudónimos de la misma parte (Chaum, (1985). Esto se llama transferencia de firmas entre seudónimos.

Cuando los seudónimos se utilizan durante el intercambio autorizado de valores, hay una serie de posibilidades para las tareas de la tercera parte integrada:

- Identificación del usuario en caso de fraude (los seudónimos están certificados y la autoridad de certificación conoce las identidades reales), es decir, no se puede garantizar la privacidad de las partes con seudónimo.
- Depósito obligatorio de pago con un depositario activo para evitar el fraude a pesar de los seudónimos completamente anónimos, es decir, se puede garantizar la privacidad de las partes con seudónimo.

Las tecnologías trilaterales de seguridad incluyen técnicas de infraestructura de claves públicas que pueden usar claves públicas certificadas, puertas de seguridad y seudónimos digitales.

Las tecnologías multilaterales sólo pueden utilizarse por un gran número de partes independientes que cooperan entre sí. Esto significa que se necesita coordinación y posiblemente negociación a gran escala. Las tecnologías multilaterales importantes para la seguridad multilateral son:

- Herramientas para negociar objetivos de protección y mecanismos de seguridad multilaterales, es decir, para el anonimato y la imposibilidad de observación.
- Mecanismos para proporcionar anonimato, imposibilidad de observación e imposibilidad de vinculación respecto a:

Todo esto sin comprometer la integridad, la disponibilidad o la responsabilidad. Las tecnologías multilaterales sólo pueden utilizarse si coopera un gran número de partes independientes.

Actualmente el eslabón más débil de la cadena de seguridad son los dispositivos de usuario, en especial su protección física y su sistema operativo.

Obviamente, la evaluación de la seguridad de las TIC y la integración de las tecnologías de seguridad son los desafíos de la investigación que tienen mayor impacto sobre la seguridad de las TIC.

Aunque debemos estar conscientes que muchas de las herramientas necesarias para lograr la seguridad pueden utilizarse también para actuar como "hackers" en sistemas inseguros, consideremos que las tecnologías de seguridad proporcionan herramientas para evitar aquellos ciberdelitos que son específicos de las redes. Hoy en día el avance tecnológico está siendo crucial y demanda que existan nuevas formas de protección que garanticen mejor la seguridad y sean sustentadas legalmente con acciones políticas para asegurar su información y pérdidas económicas.

VIOLENCIA CONTRA LA MUJER POR MEDIO DE LAS NUEVAS TECNOLOGÌAS.

Los cambios culturales y tecnológicos avanzan y desgraciadamente no a la par de la creación de normas o leyes que regulen y controlen los excesos o violación de los límites permitidos por la sociedad. El incremento de los dispositivos móviles y de la creación de redes sociales acompleja la situación para regularizar las prácticas virtuales e interacciones entre los usuarios, lo que les permite adentrarse en vivencias y experiencias desconocidas que a menudo pueden terminar de manera violenta o agresiva y que se desarrollan a través de los medios electrónicos.

El desenvolvimiento y evolución del papel de las mujeres en la sociedad ha variado, pero los estereotipos de hace cincuenta o cien años siguen afectando su paso en la sociedad, pues las siguen encasillando en los roles de cuidado y protección de los hijos y del hogar, limitándola para desenvolverse en actividades fuera de ese entorno. Esta discriminación tiene el objetivo de limitarla en su educación, en su desarrollo profesional, en su libertad sexual, entre otros.

Estas prácticas de control apoyados en las nuevas tecnologías se ha vuelto una práctica frecuente, que escudados, en algunas ocasiones, en sentimientos de celos o falso amor, les da un acceso ilimitado a las cuentas de la víctima escogida y agravan la situación de violencia de género (Castillo Vargas (s. f.).

La violencia que se da en estos entornos se adecua a las características de la violencia psicológica, afectando a las víctimas mental y emocionalmente, aunque se deba realizar una tipificación determinada para los delitos cometidos por este medio para poder crear estrategias contra los agresores y las consecuencias que implican no sólo a su persona, sino a su entorno familiar, laboral y social.

Entre los delitos de que pueden ser víctimas los niños, niñas y adolescentes se hallan la pornografía infantil, la corrupción de menores, la trata de personas, agresión, hostigamiento y acoso. Además que no existe regulación sobre los contenidos donde se ven escenas violentas o estereotipadas y el esfuerzo por promocional los derechos humanos de las mujeres y niñas no es suficiente. De hecho, consideran que son más que nada una opción para ver la perspectiva de la situación de las mujeres, la violencia que sufren y que incluso contribuye a promover dichos contenidos ofensivos, degradantes y discriminatorios (Sandoval, s. f.).

Según Castillo Vargas (s. f.), las mujeres entre las edades de 20 a 29 años son las más tendientes a caer víctimas de violencia física y sexual y en Internet varía de los 16 a los 34 años en la mayoría de las usuarias. El encontrar a los responsables se complica por la facilidad que las tecnologías permiten cuidar el anonimato de los que interactúan, pues es factible el crear una cuenta falsa en un cibercafé de acceso alejado a su entorno e iniciar un ataque bajo ese usuario inexistente a la intimidad de las victimas seleccionadas. La habilidad para dar seguimiento y localización de ciertas identidades se complica por el hecho de que la tecnología requerida para lograrlo se encuentra fuera del alcance de los usuarios cotidianos y en algunas ocasiones, de las autoridades responsables de la protección de la sociedad, y a esto se le anexa el que dentro del país, la regulación existente para penalizar las violencias cometidas a través de medios electrónicos no es suficiente. Todo esto se ve incrementado por el hecho que las usuarias no saben utilizar apropiadamente el internet y exponen su información a cualquier usuario.

El hecho de que una relación se rompa, ha sido el pretexto necesario para que los hombres descarguen toda su energía violenta sobre las mujeres que fueron su pareja apoyados en la tecnología, iniciando con su denigración,

críticas a su comportamiento, acompañados de insultos en mensajes que acosan y atosigan a las víctimas; también se pueden encargar de difundir imágenes o videos de contenido sexual o montajes elaborados con el fin de menoscabarlas.

Desgraciadamente, el contrapunto en esta situación es que la penalización por el ciberacoso puede contrarrestarse por la proclamación de la libertad de expresión que en casos como las contiendas políticas se ve implementada para continuar la denigración y ataque de las adversarias políticas y demeritar sus capacidades.

Esta propugna por regular las conductas ilícitas en el internet debe saber identificar los delitos que más se estilan para denigrar a las mujeres, y entre los que encontramos la sextorsión, en la cual una persona se hostiga amenazándola con una imagen o video de sí misma desnuda o realizando actos sexuales, que han sido compartidos previamente por medio del sexting, el cual es otros delito y consiste en enviar mensajes, imágenes y videos de contenido sexual, erótico o pornográfico usando dispositivos móviles y en el que se exponen a que sea difundido, perdiendo desde ese momento el control y dominio sobre el mismo. El ciberacoso, que ya lo mencionábamos previamente se da por el uso de información electrónica y se realiza a través de correos electrónicos, redes sociales, blogs, mensajes instantáneos, de texto, teléfonos móviles o websites de contenido difamante y degradante para asediar a alguien. En este delito, el hostigamiento consiste en enviar repetidamente la información, dañando de manera continua el bienestar de la víctima y se complementa con la multiplicidad de réplicas de dicho contenido. Este delito se ve agravado porque a niveles virtuales todos los límites de privacidad se ven eliminados y se exhiben al público, lo que incrementa en muchas ocasiones los daños, pues amigos y familiares al enterarse recrudecen e incrementan las recriminaciones hacia las mujeres que la viven, lo que consiste en una revictimización.

El resultado de experimentar todo este tipo de situaciones violatorias de sus derechos, en las mujeres mexicanas les afecta psicológicamente enormemente, pues, acorde a los estereotipos de la sociedad en que se considera que las mujeres son las que se provocan este tipo de situaciones y las culpan por la mala conducta de los agresores, enfatizado por el

desconocimiento de sus derechos y las posibilidades que existen de poder denunciar dificulta la posibilidad de manejar un registro que brinde estadísticas de agresiones de este tipo, se creen legislaciones que realmente las penalicen y se de una apropiada sanción a los agresores (Castillo Vargas (s. f.).

INSTRUMENTOS JURÍDICOS INTERNACIONALES DE PROTECCIÓN

Existen a manera de prevención distintos instrumentos internacionales que han sido creados para prevenir la violencia contra los grupos vulnerables, pero no en todos ellos se encuentran disposiciones referentes a la regulación de medios tecnológicos para prevenirla, sin embargo analizándolos se encuentran algunas regulaciones que se pueden tomar en cuenta al momento de hablar de las nuevas tecnologías, como es el caso del Pacto Internacional de Derechos Civiles y Políticos firmado en 1966 en donde su artículo 19 se enfoca sobre la libertad de expresión con las consabidas responsabilidades y deberes que aseguren el respeto a los derechos humanos y reputación de los demás, que se refuerza con el artículo 26 del mismo instrumento que habla sobre la prohibición a todo tipo de discriminación y protección igual y efectiva a todos.; la Convención sobre los Derechos del Niño con su artículo 17 en donde se pide aliciente a los medios de comunicación para difundir información y material de interés social y cultural para apoyar a los niños a desarrollarse adecuadamente, respetar los derechos humanos de otros y las libertades fundamentales, por sus padres, identidad cultural, idioma y otros para estar preparados a vivir responsablemente; la Convención Internacional sobre la Eliminación de todas las formas de Discriminación Racial no se enfoca hacia los medios de comunicación pero si solicita en su artículo 2 que se implementen todos los medios para eliminar la discriminación de todos los tipos y se solicita que los Estados se comprometan a no fomentar e incitar la discriminación y revise sus políticas gubernamentales para proteger a la ciudadanía; la Convención sobre la eliminación de todas las Formas de Discriminación contra la Mujer tampoco regula los contenidos de las nuevas tecnologías para prevenir la violencia, lo que sí enfatiza son las diferentes medidas a tomar en cuenta para erradicarla y sugiere la búsqueda de políticas que la prevengas y la eliminen; en los Estados Americanos se reconoce a la Convención

Interamericana para prevenir, sancionar y Erradicar la Violencia contra la Mujer, conocida como Convención Belém do Pará, el cual como instrumento jurídico enfocado hacia el respeto, cuidado y protección de la mujer solicita que los Estados adopten formas progresivas de medidas y programas que alienten a los medios de comunicación a crear estrategias de difusión para erradicar la violencia contra la mujer en todas sus formas y ensalzar el respeto a su dignidad, el cual se haya mas claro y definido en su artículo 8 (Centro de Estudios para el Adelanto de las Mujeres y la Equidad de Género [CEAMEG], 2011).

INSTRUMENTOS JURÍDICOS NACIONALES DE PROTECCIÓN

Dentro del país encontramos la Ley Federal de Radio y Televisión que en su artículo 5º enfatiza la función que tienen esos medios de comunicación para contribuir al respeto de los grupos vulnerables y prevenir los malos contenidos que influencien negativamente a la sociedad. Reforzando lo dicho en su artículo 63 que se refiere a la prohibición de transmisiones, imágenes, palabras, y escenas que corrompan tanto el lenguaje como las buenas costumbres, aunque no determinen específicamente la erradicación de la violencia contra las mujeres; en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia es una formalización de las presiones existentes de tipo legislativo para erradicar la violencia contra las mujeres, aunque solamente se enfoca en establecer que se vigile los medios de comunicación para que no fomenten la violencia contra las mujeres y que la Secretaría de Gobernación sancione a los medios de comunicación que no favorezcan esa erradicación; en la Ley Federal para Prevenir y Eliminar la Discriminación si se especifica que no se admite la violencia contra las mujeres a través de mensajes, imágenes en los medios de comunicación y que desconozca sus derechos y su igualdad de oportunidades; en la Ley General para la Igualdad entre Mujeres y Hombres viene derivada del artículo 4º de la Constitución Mexicana y que tiene como objetivo principal el eliminar los estereotipos de género y que en esta investigación afectan el desarrollo de las mujeres; en la Ley General de Educación además de enfocarse en desarrollar las actitudes y aptitudes de la infancia, se contempla la promoción y difusión de los derechos humanos y el respeto por sí

mismos y enfatiza la cultura de la no violencia y contempla aspectos relevantes para monitorear y limitar los contenidos en los medios de comunicación y por último, la Ley sobre Delitos de Imprenta, pero como se promulgó en 1917 y no se ha reformado no contiene ninguna regulación referente a los medios de comunicación (CEAMEG, 2011).

En el Estado de Tabasco como una estrategia para detectar los hechos delictivos cometidos por medios informáticos o electrónicos se creó a través de la Fiscalía General del Estado de Tabasco la Unidad de Investigación de Delitos Informáticos que realizará ciberpatrullaje y atención a denuncias anónimas para detectar los sitios, modus operandi y responsables de las distintas conductas delictivas para proteger niñas, niños, adolescentes y grupos vulnerables. También para orientar en la presentación de denuncias y colaborar con el Fiscal del Ministerio Público en las investigaciones (Fiscalía General del Estado de Tabasco (s. f.).

Aunque a dichas regulaciones se les han presentado iniciativas de reformas, hasta el mes de agosto de 2011, solamente dos han sido aprobadas por la Cámara de Diputados y publicadas por el Diario Oficial de la Federación, una de ellas propuso y aprobó que la Ley General de Acceso a las Mujeres a una Vida Libre de Violencia determine a los medios que organicen estrategias apropiadas para difundir, atender y prevenir la erradicación de la violencia en todas sus formas y divulgue y promueva el respeto por la mujer; la segunda se encargó de la reforma a la Ley para prevenir y sancionar la Trata de Personas que veda la divulgación y propaganda ilegal y engañosa y establece sanciones para aquellos que soliciten de forma directa o indirecta sitios para este tipo de divulgación y que tenga finalidad atraer a víctimas para trata de personas (CEAMEG, 2011).

MEDIDAS DE PROTECCIÓN EN EL USO DE REDES SOCIALES PARA LAS NIÑAS, NIÑOS Y JÓVENES, AL IGUAL QUE A LOS PADRES DE FAMILIA.

Existen miles de sugerencias para proteger a los niños y niñas en el uso de las redes sociales, pero las más importantes destacan que se debe cuidar las publicaciones que se hagan, evitando colocar el nombre completo, domicilio, número telefónico o el de las personas relacionadas a las redes. También cuidar el limitar el acceso a la información a las

personas cercanas y hacerles la misma indicación a ellos, cuidando de no usarlo como un espacio para conocer personas nuevas. El anonimato que los medios virtuales proveen pueden engañar a los usuarios y desconocer realmente con quien se está tratando. Por lo mismo, no deben confiar en lo que se platica en los chats ya que pueden inventar situaciones reales para atraer la atención y manipular fácilmente a las víctimas, por lo que el encender la webcam implica los mismos peligros de exposición. Aquellos mensajes recibidos donde ilusionan, amenazan, chantajean o intimidan o incluso ofrecen regalos, deben platicarse con familiares adultos y si hacen sentir incomodidad o miedo, pueden ser reportados en algunos sitios, que permiten identificar abusos y protegen a sus usuarios. Los comentarios incomodos o intimidatorios deben notificarse a los padres de familia para prevenirlos de la situación y tratar de configurar la privacidad de las redes para que se mantenga un control sobre lo que sucede en esos espacios virtuales (Procuraduría General de la República, (2015).

Los jóvenes aparte de las recomendaciones ya mencionadas, deben cuidar el no caer en la trampa de oferta de trabajos atractivos, más si los lugares que indican están fuera de la ciudad donde se vive y si solicitan fotografías con poca ropa; la coquetería virtual puede ser muy emocionante pero también implica involucrarse en situaciones peligrosas que tienen consecuencias nada agradables e incluso ilícitas; lo mismo se recomienda en cuanto al compartir contenido como fotos privadas solos o acompañados y se debe procurar conservar mensajes, correos electrónicos e información indebida que puedan servir como pruebas en caso de denuncia. Deben cuidar el aceptar invitaciones de personas que no conozcan personalmente y a fondo y cuidar el dar detalles de las rutinas y actividades diarias, pues todas las publicaciones realizadas no sólo se quedan en las redes sociales, sino que pueden aparecer en toda la red. Principalmente deben cuidar el crear contraseñas seguras y difíciles de identificar (Procuraduría General de la República, (2015).

Los padres de familia deben monitorear que las sugerencias antes comentadas sean respetadas por los hijos, y el no dejarlos tanto tiempo en línea sin monitoreo. Procurar enseñarles el uso apropiado y respetuoso de las redes sociales, no permitir que duerman con los dispositivos electrónicos y

explicar los riesgos del uso de internet y su navegación. Monitorear las redes de los hijos con las páginas de control existentes y establece las reglas de uso del equipo de cómputo y dispositivos y el horario de uso. Constantemente se debe monitorear el uso que ellos hacen de las redes y conocer tanto los correos electrónicos como las redes sociales y sus contraseñas.

A estas recomendaciones se pueden adjuntar muchas más, pero es importante el destacar que el internet es una herramienta que permite acceder al conocimiento de manera diligente y apropiada, siempre y cuando sepamos usarla debidamente y sepamos buscar los espacios apropiados y posteriormente, enseñar a nuestros hijos a realizar lo mismo (Procuraduría General de la República, (2015).

CONCLUSIÓN

Aunque existen legislaciones que ya toman en cuenta los delitos informáticos, aún faltan los principales y que están enfocados en la regulación de los contenidos que se comparten y que realmente respeten los derechos humanos de otros, especialmente de uno de los pertenecientes a los grupos vulnerables como son las mujeres, lo cual se enfatiza no sólo por cuestiones de miedo e ignorancia de los beneficios de la cultura de la denuncia, sino la desconfianza existente en las instituciones encargadas de aplicar las sanciones y que fallan muchas veces en garantizar la protección y el acceso a la justicia de las víctimas. Es imprescindible luchar porque el sistema se limpie y el Estado de Derecho se enfoque en la defensa de la población y sus grupos vulnerables. Que los legisladores se enfoquen en las diversas recomendaciones que los instrumentos internacionales proclaman y que propaguen y difundan la cultura del respeto a los derechos humanos y la cultura de la paz, al igual que la implementen en las legislaciones y las hagan respetar. Tabasco, no se encuentra entre los indicadores de aquellos estados del norte del país, que se destacan por un alto porcentaje de violencia contra la mujer, tal vez porque no existen muchos o porque no se implementa la cultura de la denuncia por el desconocimiento de los derechos humanos, o porque muchas de las conductas agresivas se califican como vivencias normales y que corresponden a cualquier mujer, sólo por el hecho de serlo. De ahí la importancia imperativa de luchar contra los índices existentes, y buscar la

verdadera protección de las mujeres que sólo buscan destacar en todos los ámbitos posibles, sin que sufran menoscabo o denigración de su persona cuidando la procuración y la impartición de justicia para que la aplicación sea la justa y la apropiada.

REFERENCIAS BIBLIOGRÁFICAS

Castillo Vargas, (s. f.). Violencia contra las mujeres y TIC (VCM y TIC). Fundación
Karisma. Documentos 3. Recuperado en https://karisma.org.co/wp-content/uploads/2014/12/VCMyTIC.pdf

Centro de Estudios para el Adelanto de las Mujeres y la Equidad de Género [CEAMEG], (2011). Información Analítica 2011. La violencia contra las mujeres en los medios electrónicos e impresos. Comité del Centro de Estudios para el Adelanto de las Mujeres y la Equidad de Género y la LXI Legislatura de la Cámara de Diputados. Recuperado en http://archivos.diputados.gob.mx/Centros_Estudio/ceameg/ias/Doc_30.pdf

Chaum, (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communicaciones de la ACM 24/2, 1981, pp. 84-88; p.ej. en http://world.std.com/~franl/crypto/chaum-acm-1981.html

_____, (1985). Security without Identification: Transaction Systems to make Big
Brother Obsolete; Comunicaciones de la ACM 28/10, 1985, pp. 1030-1044; http://www.chaum.com/articles/Security_Wthout_Identification.htm

Fiscalía General del Estado de Tabasco (s. f.). Unidad de Investigación de Delitos
Informáticos. Estado Libre y Soberano de Tabasco. Recuperado en http://www.fiscaliatabasco.gob.mx/Contenido/UnidadDelitosInformaticos

Pfitzmann, Schill, Westfeld, Wicke, Wolf y Zöllner, (1998). A Java-based distributed
platform for multilateral security; IFIP/GI Conferencia de Trabajo "Trends in Electronic Commerce", Hamburgo, LNCS 1402, Springer, Berlin 1998, pp. 52-64;
http://www.semper.org/sirene/publ/PSWW_98.pdf

Pfitzmann, Pfitzmann, Schunter y Waidner, (1999). Trustworthy User Devices. En: G.
Müller, K. Rannenberg (eds.): Multilateral Security in Communications, Addison-Wesley, Munich 1999, pp. 137-156. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.80.4095

Pfitzmann y Wolf, (2000), Properties of protection goals and their integration into
a user interface; Computer Networks 32, 2000, pp. 685-699. http://www.sciencedirect.com/science/article/pii/S1389128600000293

Pfitzmann, (2001). Cómo alcanzar un equilibrio entre la prevención del ciberdelito y
la privacidad. Volumen 57. Recuperado de: https://libros-revistas-derecho.vlex.es/vid/alcanzar-equilibrio-ciberdelito-privacidad-110485

Procuraduría General de la República, (2015). Fiscalía Especial para los Delitos de
Violencia contra las Mujeres y Trata de Personas. México, D. F. Recuperado en http://www.pgr.gob.mx/Fiscalias/fevimtra/Paginas/default.aspx

Sandoval, (s. f.). Los medios de comunicación en México discriminan a las mujeres:
Estudio. Animal Político. Recuperado en http://www.animalpolitico.com/2012/03/los-medios-de-comunicacion-en-mexico-discriminan-a-las-mujeres-estudio-legislativo/